

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM

Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICH NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

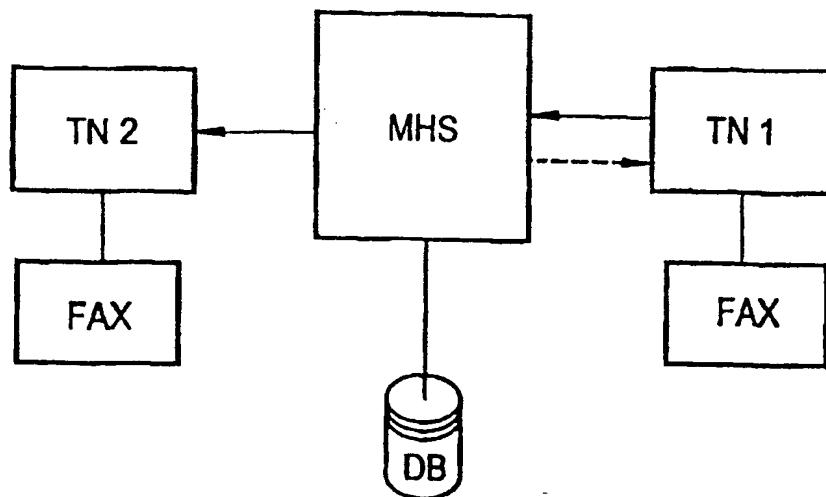
(51) Internationale Patentklassifikation <sup>6</sup> : <b>H04L 12/58, 29/06</b>	A1	(11) Internationale Veröffentlichungsnummer: <b>WO 99/08424</b>  (43) Internationales Veröffentlichungsdatum: <b>18. Februar 1999 (18.02.99)</b>
(21) Internationales Aktenzeichen: <b>PCT/DE98/02031</b>	(81) Bestimmungsstaaten: US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) Internationales Anmeldedatum: <b>20. Juli 1998 (20.07.98)</b>	Veröffentlicht <i>Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>	
(30) Prioritätsdaten: 197 34 069.5      6. August 1997 (06.08.97)      DE		
(71) Anmelder ( <i>für alle Bestimmungsstaaten ausser US</i> ): SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacher Platz 2, D-80333 München (DE).		
(72) Erfinder; und		
(75) Erfinder/Anmelder ( <i>nur für US</i> ): WOLF, Hans-Hermann [DE/DE]; Schildensteinstrasse 12, D-81673 München (DE).		
(74) Gemeinsamer Vertreter: SIEMENS AG; Postfach 22 16 34, D-80506 München (DE).		

(54) Title: METHOD AND DEVICE FOR GENERATING INFORMATION ON MESSAGES TRANSMITTED

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR GENERIERUNG VON INFORMATIONEN ÜBER VERSENDETE NACHRICHTEN

(57) Abstract

The invention relates to a method for data transmission between a sender (TN1) and a receiver (TN2) in a communications network. Once a message has been transmitted to a receiver, the sender is issued an acknowledgment by a central office (MHS) of said communications network. To this end, the message transfer is managed by a central entity (MHS), which ensures that the message is transmitted to the receiver (TN2) and issues an acknowledgment to the sender (TN1) of said message once the transmission has taken place.



(57) Zusammenfassung

Verfahren in einem Kommunikationsnetz zur Nachrichtenübertragung zwischen einem Sender (TN1) und einem Empfänger (TN2), wobei dem Sender nach erfolgter Übertragung einer Nachricht an den Empfänger mittels eines in diesem Kommunikationsnetz vorgesehenen zentralen Dienstes (MHS) eine Empfangsbestätigung zur Verfügung gestellt wird. Diese Aufgabe wird gelöst, indem der Nachrichtentransfer über eine zentrale Instanz (MHS) geleitet wird. Diese Instanz stellt die Auslieferung der Nachricht an einen Empfänger (TN2) sicher und generiert nach erfolgter Auslieferung eine Bestätigung für den Sender (TN1) dieser Nachricht.

**LEDIGLICH ZUR INFORMATION**

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Amenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolci	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Verfahren und Vorrichtung zur Generierung von Informationen über versendete Nachrichten

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur  
5 Bestätigung des Empfangs von in einem Kommunikationsnetz ver-  
sendeten Nachrichten durch einen zentralen Dienst.

In Kommunikationsnetzen hat der Sender einer Nachricht keine  
Möglichkeit zu beweisen, daß eine von ihm versendete  
10 Nachricht auch beim Empfänger angekommen ist. Oftmals ist  
eine solche Bestätigung aber notwendig, wenn etwa bestimmte  
Fristen einzuhalten sind. Daher müssen beispielsweise  
Schriftstücke über den langsamen und teuren Weg der Briefpost  
(Einschreiben mit Rückschein) versendet werden, da bei der  
15 Versendung beispielsweise mittels eines Faxgerätes oder eines  
Computers nur eine Information über das Absenden der  
Nachricht generiert wird, nicht aber über deren Empfang.  
Im Falle von elektronischer Post ist es bei manchen Systemen,  
wie beim Message Handling System X.400 möglich, eine  
20 Empfangsbestätigung zu verlangen ('proof of delivery',  
'content integrity'). Hier wird die Bestätigung vom Message  
Storage MS des Empfängers generiert und an den Sender über-  
mittelt, sobald der MS die Nachricht dem Empfänger zustellen  
konnte. Diese Empfangsbestätigungen haben jedoch keinerlei  
25 Beweiskraft und werden immer an den Absender der Nachricht  
gesendet.  
Bei Nachrichten in einem anderen Format (beispielsweise  
Sprache) existiert bis zum heutigen Tag keine Möglichkeit der  
Bestätigung.

Aufgabe der Erfindung ist es, eine technische Lehre für die Generierung einer beweiskräftigen Information den Empfang einer Nachricht für den Sender dieser Nachricht in einem Kommunikationsnetz anzugeben.

5

Diese Aufgabe wird durch ein Verfahren gemäß Anspruch 1 und eine Vorrichtung gemäß Anspruch 7 gelöst, indem der Nachrichtentransfer über eine zentrale Instanz geleitet wird.

Diese Instanz stellt die Auslieferung der Nachricht an einen  
10 Empfänger sicher und generiert nach erfolgter Auslieferung  
eine Bestätigung für den Sender dieser Nachricht. Diese  
Lösung beinhaltet mehrere Vorteile: die Versendung von wichtigen  
Nachrichten kann deutlich schneller und kostengünstiger  
geschehen, als dies bislang möglich war. Der Sender kann  
15 diese Informationen anfordern unabhängig von den verwendeten  
Endgeräten auf Sender- oder Empfängerseite und die Nachricht  
kann in einem beliebigen Format übersendet werden.

Vorteilhafte Ausgestaltungen und Weiterbildungen sind in den  
20 Unteransprüchen angegeben.

Im folgenden wird der Begriff Intelligentes Netz verwendet  
für ein Kommunikationsnetz, das geeignete Netzelemente enthält,  
die vordefinierte Dienste ausführen können.

25 Der Begriff Signatur kennzeichnet eine Zeichenfolge, die zum  
Beweis der Authentizität des Inhalts dieser Datei geeignet  
ist, beispielsweise eine Zeichenfolge, die mittels einer  
Funktion aus einer Binärdatei und einem (privaten) Schlüssel  
generiert werden kann.

Im folgenden wird die Erfindung anhand von Ausführungsbeispielen erläutert.

Dabei zeigt

- 5 Figur 1 den prinzipiellen Aufbau eines Kommunikationsnetzes mit einem zentralen Dienst (MHS, Message Handling System und DB, Datenbank) gemäß Anspruch 1,
- Figur 2 ein Beispielhaftes Intelligentes Netz, welches eine zentrale Instanz IP (Intelligent Peripheral) verwendet, um
- 10 erfindungsgemäß Information über eine versendete Nachricht vom Sender (Teilnehmer TN 1) zu einem Empfänger (Teilnehmer TN 2) zu generieren und an den Sender TN 1 zu versenden.
- Figur 3 zeigt eine Beispielhafte Übertragung einer Nachricht (FAX) in einem intelligenten Netz (IN), wobei der Sender
- 15 (TN 1) nach erfolgter Übertragung der Nachricht an einen Empfänger (TN B) von einem zentralen Diensterbringer (IP) eine Bestätigung (ACK) bekommt.
- Die Information, die über eine versendete Nachricht generiert
- 20 und gespeichert oder an den Sender dieser Nachricht gesendet werden soll, kann verschiedene Ausprägungen beinhalten. Neben Sender, Empfänger und Sendezeitpunkt können weitere Informationen enthalten sein, wie Übertragungsweg, Übertragungsdauer, der Inhalt der gesendeten Nachricht, zusätzliche
- 25 Kommentare des Senders oder eine Zeichenfolge (Signatur), die den Inhalt und den Absender der Nachricht eindeutig identifiziert. Es kann auch eine Signatur durch den zentralen Dienst angefügt werden, der verhindert, daß der Inhalt der Information nachträglich verändert wird. Diese Signatur kann
- 30 beispielsweise mittels Authentifizierungsprozeduren laut

ITU-T X.509 generiert werden. Der Erzeuger der Signatur verwendet hierfür seinen geheimen Schlüssel und eine Hash-Funktion, der Empfänger kann die Signatur mittels des öffentlichen Schlüssels des Senders und der Hash-Funktion verifi-  
5 zieren.

Weiterhin kann diese Information zentral gespeichert und nur bei Bedarf abgerufen werden oder nach Auslieferung der Nachricht sofort an den Sender der Nachricht ausgeliefert werden.  
10 Es ist auch möglich, die Informationen zu sammeln und zusammen in einer 'Abrechnung' nach Ablauf einer Frist zuzustellen, oder die Information nach einer bestimmten Zeit wieder zu löschen, wenn sie bis dahin vom Sender nicht angefordert wurde. Es ist ebenfalls denkbar, daß die Information über die Nachrichtenübertragung nicht dem Sender dieser Nachricht  
15 sondern einem anderen Teilnehmer (beispielsweise dem Empfänger) in diesem Kommunikationsnetz zugestellt wird.

In dem beispielhaften Aufbau wie in Figur 1 beschrieben ist das MHS in einem PABX oder im öffentlichen Netz auf einem  
20 IN/SN/ESP anzusiedeln. Ein denkbarer Anwendungsfall besteht darin, daß das Faxgerät des angerufenen Teilnehmers TN 2 räumlich entfernt steht. Der Teilnehmer TN 2 kann dann über den Empfang eines Faxes zum Beispiel mittels einer Ansage 'Fax von ... eingetroffen' über sein Telefon informiert  
25 werden.

Figur 2 zeigt eine beispielhafte Lösung der Aufgabe in Form eines zentralen Dienstes in einem Intelligenten Netz IN. Physikalisch befindet sich der Dienst auf einem Netzelement  
30 mit Namen Intelligent Peripheral IP. Sender (Teilnehmer TN 1)

und Empfänger (TN 2) der Nachricht sind jeweils über eine Vermittlungsstelle (Service Switching Point, SSP 1 und SSP 2) mit dem Kommunikationsnetz verbunden. Das zentrale Managementsystem (Service Management System SMS) verwaltet alle  
5 Dienstaufrufe, die in diesem Kommunikationsnetz auftreten und mit Hilfe des Dienstesteuerungssystems (Service Control Point SCP) wird das für das Generieren und Speichern der Informationsdaten zuständige Netzelement (IP) ermittelt und die Vermittlungsstelle des Senders angewiesen mit dem IP in  
10 Verbindung zu treten.

Dabei wählt der Sender TN 1 eine 'IN Nummer' für den Nachrichten-Service mit Empfangsbestätigung. Der SCP fordert die Zielrufnummer des Kommunikationsendgerätes (beispielsweise Faxgerät) des Empfängers TN 2 bei TN 1 an, sofern diese aus  
15 dem Aufruf von TN 1 nicht bereits hervorgeht. Abhängig von der Verfügbarkeit des Services auf IP/SN sowie der Lokalität von TN 2 wird ein IP/SN ausgewählt. Der IP/SN kontrolliert und steuert die Nachrichtenübertragung und sorgt bei erfolgreicher Übertragung für die Bereitstellung (und eventuell  
20 Übertragung) der Empfangsbestätigung.

Figur 3 zeigt eine beispielhafte Übertragung einer Nachricht in Form eines Faxes über ein Intelligentes Netz, dessen Struktur in Figur 2 bereits erläutert wurde. Der Sender der  
25 Nachricht (Teilnehmer TN A) sendet seine Nachricht an die nächstgelegene Vermittlungsstelle (Service Switching Point, SSP1). Da der Sender einen zentralen Dienst angefordert hat, wird die Anfrage an eine zentrale Dienstesteuerung (Service Control Point SCP) weitergeleitet und die Vermittlungsstelle  
30 SSP1 erhält Instruktionen zum weiteren Vorgehen, insbesondere

den Ort, an dem der zentrale Dienst ausgeführt wird (Intelligent Peripheral IP). Dorthin leitet der SSP1 die Nachricht weiter. Der IP wiederum sendet die Nachricht an die nächstegelegene Vermittlungsstelle des Empfängers (SSP2). Er  
5 behält eine Kopie der Nachricht und wartet auf eine Empfangsmeldung durch den Empfänger (Teilnehmer TN B). Sobald diese eintrifft, generiert IP einen Datensatz, der alle Informationen enthält, die vom Sender angefordert wurden. Abhängig von den Anforderungen des Senders wird dieser bei-  
10 spielsweise in einer zentralen Datenbank abgelegt. Weiterhin kann eine Mitteilung an den Sender der ursprünglichen Nachricht weitergeleitet werden. Mit dem Eintreffen der Bestätigung beim Sender der Nachricht ist der Vorgang beendet.

## Abkürzungsverzeichnis:

ACK	Acknowledgement
DB	Datenbank
ESP	Enhanced System Platform
5 FAX	Nachricht
IN	Intelligent Network
INSTR	Instruction
IP	Intelligent Peripheral
MHS	Message Handling System
10 PABX	Private Automatic Branch Exchange
REQ	Request
SCP	Service Control Point
SMS	Service Management System
SN	Service Node
15 SSP	Service Switching Point
TN	Teilnehmer

## Literaturverzeichnis:

20 X.400	CCITT Recommendation X.400, Message Handling Services: Message Handling System and Service Overview (3/93)
25 X.509	ITU-T X.509 Information Technology - Open Systems Interconnection - The Directory: Authentication Framework (11/93)

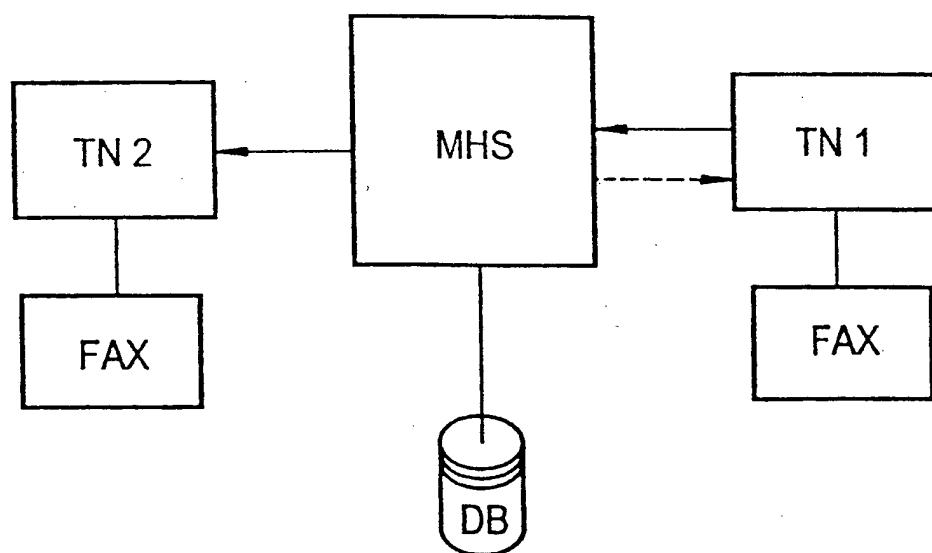
**Patentansprüche**

1. Verfahren in einem Kommunikationsnetz zur Nachrichtenübertragung zwischen einem Sender und einem Empfänger, wobei dem Sender nach erfolgter Übertragung einer Nachricht an den Empfänger mittels eines in diesem Kommunikationsnetz vorgesehenen zentralen Dienstes eine Empfangsbestätigung zur Verfügung gestellt wird.
- 10 2. Verfahren nach Anspruch 1, wobei die Empfangsbestätigung nach Auslieferung der Nachricht dem Sender der Nachricht zugestellt wird.
- 15 3. Verfahren nach einem der vorherigen Ansprüche, wobei dem Sender nach Übertragung der Nachricht an einen Empfänger eine Empfangsbestätigung zugestellt wird, die eine Symbolfolge enthält, welche zur Beweisführung über den Inhalt der Nachricht dienen kann.
- 20 4. Verfahren nach einem der vorherigen Ansprüche, wobei dem Sender nach Übertragung der Nachricht an einen Empfänger eine Empfangsbestätigung zugestellt wird, die den Inhalt der empfangenen Nachricht enthält.
- 25 5. Verfahren nach einem der vorherigen Ansprüche, wobei der zentrale Dienst eine Empfangsbestätigung generiert, die eine zusätzliche Authentifizierung des zentralen Dienstes enthält, von dem die Empfangsbestätigung generiert wurde.

6. Verfahren nach Anspruch 1, wobei der Sender auswählen kann, welche Angaben die Bestätigung enthält.
7. Verfahren nach einem der vorigen Ansprüche, wobei die 5 Bestätigung auch einem anderen Teilnehmer in diesem Kommunikationsnetz zur Verfügung gestellt wird.
8. Vorrichtung in einem Kommunikationsnetz mit Mitteln zum Empfangen einer Nachricht und Mitteln zum Erzeugen einer 10 Empfangsbestätigung.
9. Vorrichtung nach Anspruch 7 mit Mitteln zum Senden einer Empfangsbestätigung an den Sender einer Nachricht.
- 15 10. Vorrichtung nach den Ansprüchen 7 oder 8 mit Mitteln zum Erzeugen einer Symbolfolge, welche zur Beweisführung über den Inhalt der Nachricht dienen kann.

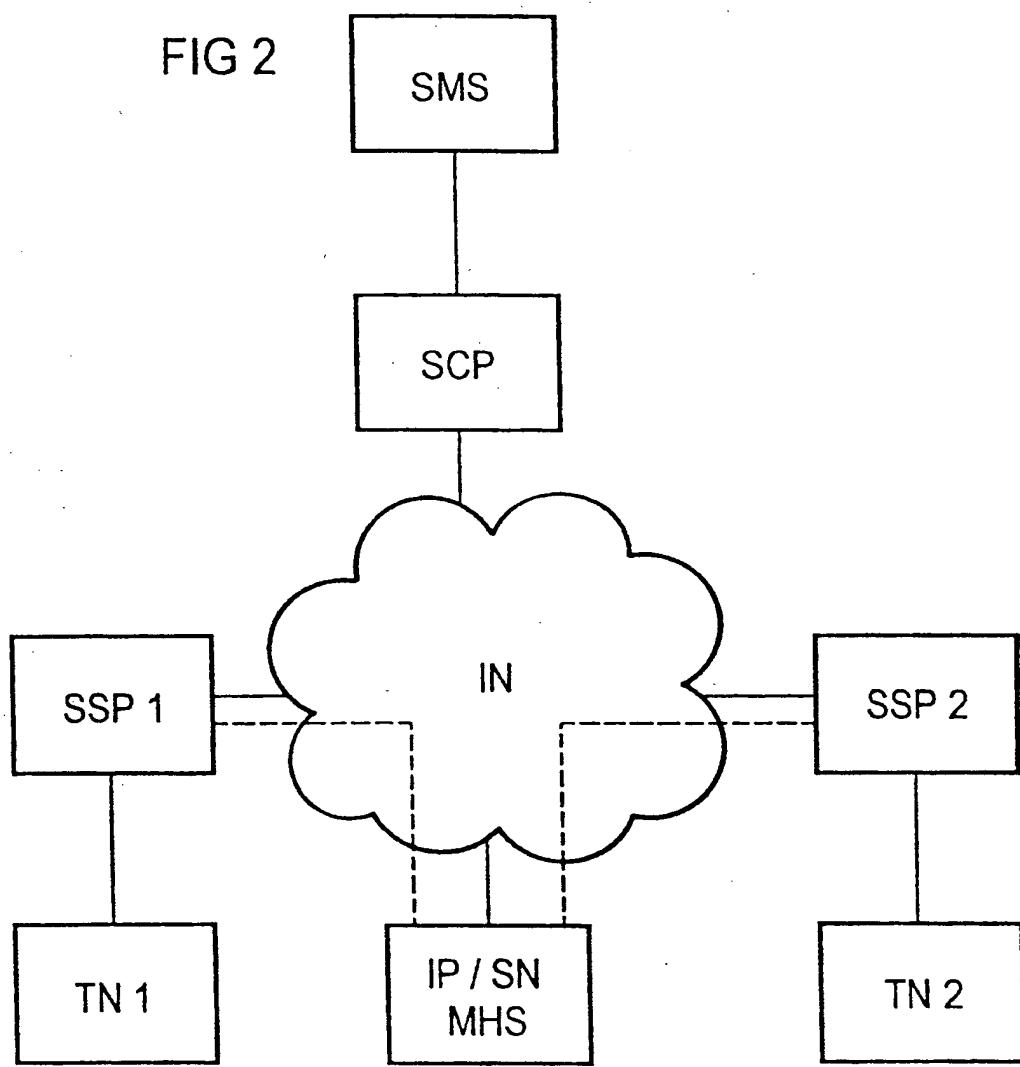
1 / 3

FIG 1



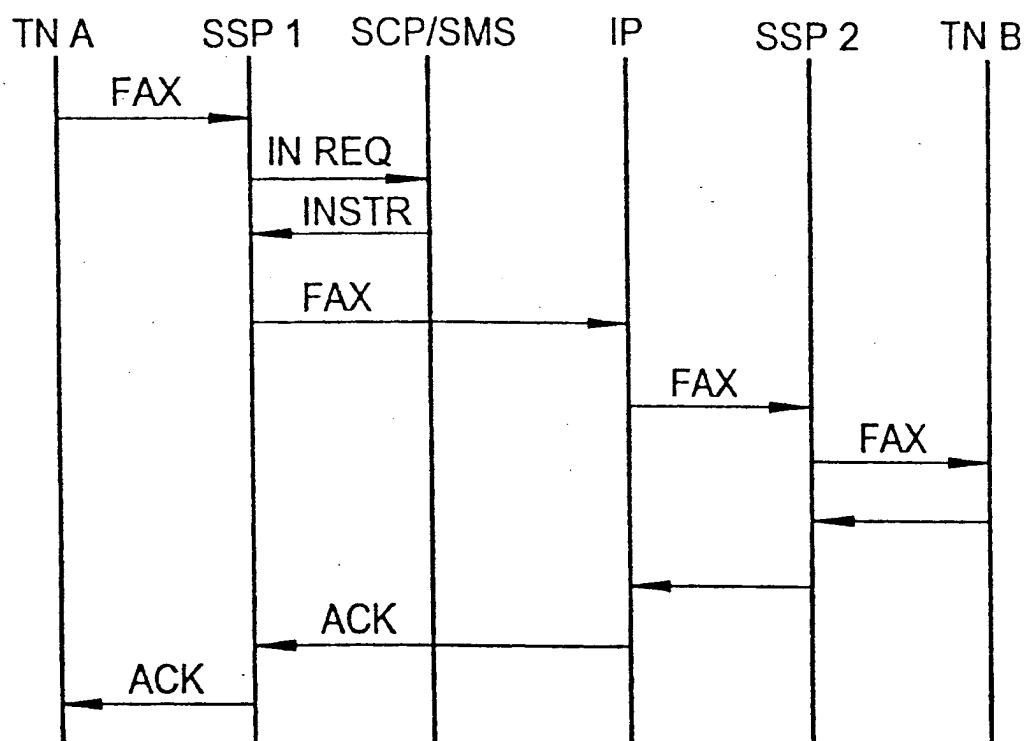
2 / 3

FIG 2



3 / 3

FIG 3



# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/DE 98/02031

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 6 H04L12/58 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 38987 A (SLOO MARSHALL A) 5 December 1996	1,2,4, 6-9
Y	see page 5, line 12 - line 18 see page 8, line 13 - page 13, line 7 ---	3,5,10
Y	TOUCH J D: "PERFORMANCE ANALYSIS OF MD5" COMPUTER COMMUNICATIONS REVIEW, vol. 25, no. 4, 1 October 1995, pages 77-86, XP000541653 see page 77, right-hand column, line 45 - page 78, left-hand column, line 8 --- -/-	3,10

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the International filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the International search

Date of mailing of the International search report

11 January 1999

27/01/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3018

Authorized officer

Ströbeck, A

# INTERNATIONAL SEARCH REPORT

In. National Application No  
PCT/DE 98/02031

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MITCHELL C ET AL: "CCITT/ISO STANDARDS FOR SECURE MESSAGE HANDLING" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 7, no. 4, May 1989, pages 517-524, XP000007972 see page 518, right-hand column, line 28 - page 519, left-hand column, line 12 -----	5

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 98/02031

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9638987 A	05-12-1996	AU 5883896 A	18-12-1996

# INTERNATIONALER RECHERCHENBERICHT

b nationales Aktenzeichen  
PCT/DE 98/02031

<b>A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES</b> IPK 6 H04L12/58 H04L29/06																			
<p>Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK</p> <p><b>B. RECHERCHIERTE GEBIETE</b></p> <p>Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationsymbole ) IPK 6 H04L</p> <p>Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen</p> <p>Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)</p>																			
<p><b>C. ALS WESENTLICH ANGESEHENE UNTERLAGEN</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Kategorie*</th> <th style="width: 80%;">Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile</th> <th style="width: 10%;">Betr. Anspruch Nr.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>WO 96 38987 A (SLOO MARSHALL A) 5. Dezember 1996</td> <td>1,2,4, 6-9</td> </tr> <tr> <td>Y</td> <td>siehe Seite 5, Zeile 12 - Zeile 18 siehe Seite 8, Zeile 13 - Seite 13, Zeile 7</td> <td>3,5,10</td> </tr> <tr> <td>Y</td> <td>TOUCH J D: "PERFORMANCE ANALYSIS OF MD5" COMPUTER COMMUNICATIONS REVIEW, Bd. 25, Nr. 4, 1. Oktober 1995, Seiten 77-86, XP000541653 siehe Seite 77, rechte Spalte, Zeile 45 - Seite 78, linke Spalte, Zeile 8</td> <td>3,10</td> </tr> <tr> <td></td> <td style="text-align: center;">---</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;">-/--</td> <td></td> </tr> </tbody> </table>		Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.	X	WO 96 38987 A (SLOO MARSHALL A) 5. Dezember 1996	1,2,4, 6-9	Y	siehe Seite 5, Zeile 12 - Zeile 18 siehe Seite 8, Zeile 13 - Seite 13, Zeile 7	3,5,10	Y	TOUCH J D: "PERFORMANCE ANALYSIS OF MD5" COMPUTER COMMUNICATIONS REVIEW, Bd. 25, Nr. 4, 1. Oktober 1995, Seiten 77-86, XP000541653 siehe Seite 77, rechte Spalte, Zeile 45 - Seite 78, linke Spalte, Zeile 8	3,10		---			-/--	
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.																	
X	WO 96 38987 A (SLOO MARSHALL A) 5. Dezember 1996	1,2,4, 6-9																	
Y	siehe Seite 5, Zeile 12 - Zeile 18 siehe Seite 8, Zeile 13 - Seite 13, Zeile 7	3,5,10																	
Y	TOUCH J D: "PERFORMANCE ANALYSIS OF MD5" COMPUTER COMMUNICATIONS REVIEW, Bd. 25, Nr. 4, 1. Oktober 1995, Seiten 77-86, XP000541653 siehe Seite 77, rechte Spalte, Zeile 45 - Seite 78, linke Spalte, Zeile 8	3,10																	
	---																		
	-/--																		
<input checked="" type="checkbox"/> Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen <input checked="" type="checkbox"/> Siehe Anhang Patentfamilie																			
<p>* Besondere Kategorien von angegebenen Veröffentlichungen :      "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist      "E" älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldeatum veröffentlicht worden ist      "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)      "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht      "P" Veröffentlichung, die vor dem Internationalen Anmeldeatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist</p> <p>"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldeatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist      "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindenderischer Tätigkeit beruhend betrachtet werden      "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindenderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist      "&amp;" Veröffentlichung, die Mitglied derselben Patentfamilie ist</p>																			
Datum des Abschlusses der Internationalen Recherche  11. Januar 1999																			
Absendedatum des Internationalen Recherchenberichts  27/01/1999																			
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016																			
Bevollmächtigter Bediensteter  Ströbeck, A																			

# INTERNATIONALER RECHERCHENBERICHT

In nationales Aktenzeichen  
PCT/DE 98/02031

## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	MITCHELL C ET AL: "CCITT/ISO STANDARDS FOR SECURE MESSAGE HANDLING" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Bd. 7, Nr. 4, Mai 1989, Seiten 517-524, XP000007972 siehe Seite 518, rechte Spalte, Zeile 28 - Seite 519, linke Spalte, Zeile 12 -----	5

**INTERNATIONALER RECHERCHENBERICHT**

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

In. nationales Aktenzeichen

PCT/DE 98/02031

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9638987 A	05-12-1996	AU 5883896 A	18-12-1996